الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1234

(2022/01)

السلسلة X: شبكات البيانات والاتصالات،
بين الأنظمة المفتوحة ومسائل الأمن

أمن الفضاء السيبراني– مكافحة الرسائل الاقتحامية

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية الموجهة عبر خدمة الرسائل متعددة الوسائط

التوصية ITU-T X.1234

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات، بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	X.1030–X.1049
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب (1)	X.1140–X.1149
أمن التطبيقات (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	**X.1230-X.1249**
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1350–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1399
أمن سجل الحسابات الموزع (DLT)	X.1400–X.1429
أمن التطبيقات (2)	X.1450–X.1459
أمن الويب (2)	X.1470–X.1489
تبادل معلومات الأمن السيبراني	
نظرة عامة على الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
الدفاع السيبراني	X.1590–X.1599
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699
الاتصالات الكمومية	
المصطلحات	X.1700–X.1701
المولد الكمومي للأعداد العشوائية	X.1702–X.1709
إطار أمن شبكات توزيع المفاتيح الكمومية (QKDN)	X.1710–X.1711
التصميم الأمني للشبكات QKDN	X.1712–X.1719
التقنيات الأمنية للشبكات QKDN	X.1720–X.1729
أمن البيانات	
أمن البيانات الضخمة	X.1750–X.1759
حماية البيانات	X.1770–X.1789
أمن الاتصالات المتنقلة الدولية-2020	X.1800–X.1819

لمزيد من التفاصيل يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصية ITU-T X.1234

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية الموجهة عبر خدمة الرسائل متعددة الوسائط

ملخص

تحدد التوصية ITU-T X.1234 مبادئ توجيهية لمكافحة الرسائل الاقتحامية الموجهة عبر خدمة الرسائل متعددة الوسائط (MMS). وتحلل السيناريوهات والخصائص وأساليب التعرف النموذجية على هذه الرسائل الاقتحامية وتحدد الإطار التقني ومسارات العمل وبعض التكنولوجيات الرئيسية للتعرف عليها لمساعدة مقدمي الخدمة ومستعمليها على مكافحتها.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1234	2022-01-07	17	11.1002/1000/14796

مصطلحات أساسية

خدمة الرسائل متعددة الوسائط، رسائل اقتحامية موجهة عبر خدمة الرسائل متعددة الوسائط، إطار تقني

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تُعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يلزم" وصيغ ملزمة أخرى مثل فعل "يجب" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات/حقوق ملكية برمجيات، يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قواعد البيانات المناسبة لدى قطاع تقييس الاتصالات المتاحة في الموقع الإلكتروني للقطاع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

مقدمة

خدمة الرسائل متعددة الوسائط (MMS) طريقة معيارية لإرسال رسائل تتضمن محتوى متعدد الوسائط من وإلى هاتف متنقل عبر شبكة خلوية. ويمكن أن يشير المستخدمون والموردون إلى هذه الرسالة كصورة ومقطع فيديو وصوت ورسوم متحركة وما إلى ذلك. ومع تطور تكنولوجيا الاتصالات وزيادة شعبية الهواتف الذكية، أصبحت خدمة الرسائل متعددة الوسائط وسيلة رئيسية لإرسال الرسائل، لا سيما بالنسبة للشباب وشركات وسائط الإعلام التي تستخدم هذه التكنولوجيا على أساس تجاري كوسيلة لتقديم الأخبار والمحتوى الترفيهي. وتتيح خدمة الرسائل متعددة الوسائط إقامة تواصل اجتماعي ملائم وإرسال رسائل ذات ألوان زاهية، ولكنها تصبح أيضاً طريقة للمقتحمين لإرسال رسائل اقتحامية MMS. وأصبحت هذه الرسائل الاقتحامية MMS بما فيها الإعلانات غير المتوقعة، ومعلومات الاحتيال، والفيروسات، مشكلة واسعة الانتشار وتتسبب في خسارة فادحة في إيرادات مشغلي الاتصالات ومقدمي الخدمات والمستعملين.

ولذلك أصبحت مكافحة الرسائل الاقتحامية الموجهة عبر الرسائل متعددة الوسائط مكافحة فعالة اتجاهاً مهماً في مجال تكنولوجيا مكافحة الرسائل الاقتحامية.

التوصية ITU-T X.1234

مبادئ توجيهية بشأن مكافحة الرسائل الاقتحامية الموجهة عبر خدمة الرسائل متعددة الوسائط

1 مجال التطبيق

تقترح هذه التوصية إطاراً تقنياً لمكافحة الرسائل الاقتحامية الموجهة عبر الرسائل متعددة الوسائط لتحقيق إدارة الرسائل الاقتحامية MMS والتحكم فيها. ويحدد هذا الإطار المكونات الوظيفية ومسارات العمل وبعض التكنولوجيات الرئيسية للتعرف على الرسائل الاقتحامية MMS. وبالإضافة إلى ذلك، تتناول هذه التوصية سيناريوهات نموذجية للرسائل الاقتحامية MMS مع تحليل لأنواع مختلفة من الرسائل الاقتحامية MMS وخصائصها العامة.

وجدير بالإشارة إلى أن جميع العمليات الواردة في هذه التوصية يجب أن يسمح بها المستعملون واللوائح الإدارية. وينبغي أن تتبع العملية برمّتها التشريعات المعمول بها بعناية تفادياً لانتهاك خصوصية المستعملين.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية.

والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.1231] التوصية ITU-T X.1231 (2008)، *الاستراتيجيات التقنية لمكافحة الرسائل الاقتحامية*.

[ITU-T X.1247] التوصية ITU-T X.1247 (2016)، *إطار تقني لمكافحة الرسائل الاقتحامية المتنقلة*.

3 التعاريف

1.3 مصطلحات معرَّفة في مواضع أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في مواضع أخرى:

1.1.3 خدمة الرسائل متعددة الوسائط (multimedia messaging service) (MMS) [ITU-T X.1231]: تشير خدمة الرسائل متعددة الوسائط إلى نوع من أنواع خدمة الرسائل اللاحقة لخدمة الرسائل القصيرة (SMS) والتي بإمكانها نقل مختلف الرسائل متعددة الوسائط، بما فيها النصوص والرسوم والصوت والفيديو وغير ذلك، من خلال شبكة متنقلة أو شبكة لاسلكية أو شبكة ثابتة.

2.1.3 رسائل اقتحامية موجهة عبر خدمة الرسائل متعددة الوسائط (multimedia message service spam) (MMS) [ITU-T X.1247]: رسائل اقتحامية موجهة عبر خدمة الرسائل متعددة الوسائط.

3.1.3 صاحب الرسائل الاقتحامية (spammer) [ITU-T X.1231]: يشير صاحب الرسائل الاقتحامية إلى كيان أو شخص ينشئ رسائل اقتحامية ويرسلها.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلح التالي:

1.2.3 وظائف التعرف على الرسائل الاقتحامية الموجهة عبر الرسائل متعددة الوسائط (MMSSIF): نظام لمكافحة الرسائل الاقتحامية MMS مستقل عن مركز خدمة الرسائل متعددة الوسائط (MMSC) الذي يشمل المكونات الوظيفية التالية: وظيفة المراقبة ووظيفة حيازة البيانات ووظيفة المعالجة المسبقة ووظيفة التعرف ووظيفة التخلص ووظيفة التفعيل ووظيفة إدارة النظام.

4 الاختصارات والأسماء المختصرة

تستعمل هذه التوصية الاختصارات والأسماء المختصرة التالية:

ASR التعرف التلقائي على الكلام (*Automatic Speech Recognition*)

MMS خدمة الرسائل متعددة الوسائط (*Multimedia Message Service*)

MMSC مركز خدمة الرسائل متعددة الوسائط (*Multimedia Message Service Centre*)

MMSSIF وظيفة التعرف على الرسائل الاقتحامية الموجهة عبر خدمة الرسائل متعددة الوسائط (*Multimedia Message Service Spam Identification Function*)

SMS خدمة الرسائل القصيرة (*Short Message Service*)

UICC بطاقة الدوائر المتكاملة الشاملة (*Universal Integrated Circuit Cards*)

URL موقع الموارد الموحَّد (*Uniform Resource Location*)

5 الاصطلاحات

تستعمل هذه التوصية الاصطلاحات التالية:

تدل كلمة "**ينبغي**" على مطلب يوصى به لكنه غير إلزامي مطلقاً. وبالتالي لا يتعين توفر هذا المتطلب لزعم الامتثال.

وتدل كلمة "**يجوز**" على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به.

وفي متن هذه التوصية، تظهر كلمة "**يمكن**" أحياناً وفي هذه الحالة يجب تفسيرها على أنها تعني "**يستطيع**".

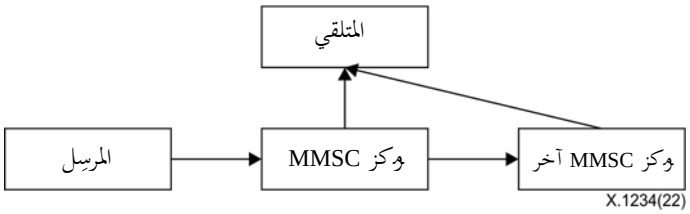
6 نظرة عامة

تشير خدمة الرسائل متعددة الوسائط إلى نوع من أنواع خدمة الرسائل المقدمة بعد خدمة الرسائل القصيرة (SMS) والتي بإمكانها نقل مختلف الرسائل متعددة الوسائط، بما فيها النصوص والرسوم والصوت والفيديو من خلال شبكات متنقلة أو شبكات قائمة على بروتوكول الإنترنت. ومع تكنولوجيات الاتصالات والإنترنت سريعة التطور، فضلاً عن سرعة نمو شعبية الهواتف الذكية، تعد الرسائل متعددة الوسائط التي تتيح إقامة تواصل اجتماعي مناسب وإرسال رسائل ذات ألوان زاهية، وسيلة مهمة لإرسال الرسائل، ولا سيما بالنسبة للشباب وشركات وسائط الإعلام التي تستخدمها على أساس تجاري كوسيلة لتقديم الأخبار ومحتوى ترفيهي.

ومع ذلك، من الممكن أيضاً لمرسلي الرسائل الاقتحامية إرسال رسائل اقتحامية عبر خدمة الرسائل متعددة الوسائط. وأصبحت الرسائل الاقتحامية MMS بما في ذلك المعلومات غير المرغوبة، مثل الإعلانات، والاحتيال، والفيروسات، والرسائل المزعجة، مشكلة واسعة الانتشار وتتسبب في خسارة فادحة في إيرادات مشغلي الاتصالات ومقدمي الخدمات والمستعملين. ولذلك، أصبحت كيفية مكافحة الرسائل الاقتحامية MMS بشكل فعال من الناحية التقنية تحدياً هاماً في مجال مكافحة الرسائل الاقتحامية.

7 سيناريوهات وخصائص الرسائل الاقتحامية MMS

كما هو موضح في الشكل 7-1، ينطوي إجراء الرسائل متعددة الوسائط على ثلاث خطوات رئيسية كالتالي: (1) يُعدّ المرسِل محتوى MMS ويرسله إلى المركز MMSC، الذي تنتمي إليه بطاقة الدارة المتكاملة الشاملة (UICC) الخاصة به؛ (2) يتلقى المركز MMSC المحتوى MMS الذي أرسله المرسِل ويقرر ما إذا كان سيرسل رسالة الوسائط المتعددة إلى المركز MMS التالي أو إلى المتلقي مباشرة؛ (3) يحصل المتلقي على رسالة الوسائط المتعددة من المركز MMSC الذي قد يكون مختلفاً عن المركز MMSC الذي استخدمه المرسِل.



الشكل 7-1 – إجراء الرسائل متعددة الوسائط

يستخدم المقتحمون الإجراء المذكور أعلاه لإرسال رسائل اقتحامية إلى المستعملين وهو أمر مزعج للغاية وقد يتسبب للمستعملين في فقدان فوائد. وقد يكون محتوى الرسائل الاقتحامية إعلانياً أو احتيالياً، وما إلى ذلك. وفيما يلي بعض السيناريوهات النموذجية للرسائل الاقتحامية MMS:

1 رسائل اقتحامية احتيالية: هي رسائل اقتحامية MMS تستخدم الحجج لإقناع متلقيها بإمكانية الحصول على بعض الفوائد أو بأن شيئاً ما صحيح. وإذا أجاب المتلقي على النحو المبين في الرسالة، ستُفرض رسوم عليه أو سيُسجل في نوع من خدمات القيمة المضافة التي تقدمها شركة الاحتيال مقابل الدفع.

2 رسائل اقتحامية تسللية: تحمل بعض الرسائل الاقتحامية MMS ملف وسائط تسللية، وبمجرد العثور على هاتف محمول معرض للخطر، وقيام مستعمل الهاتف بفتح ملف الوسائط، يحصل مُرسِل الرسالة الاقتحامية على أعلى إذن إداري لنظام الهاتف، ومن ثم قد تتعرض جميع المعلومات السرية الموجودة في الهاتف للسرقة، دون أن يدرك المتلقي تماماً حدوث ذلك.

3 رسالة اقتحامية فيروسية: يمكن أن تحتوي رسالة اقتحامية MMS على نوع معين من أنواع ملف إعداد الفيروسات الذي يبدو كأنه ملف عادي. وبمجرد أن ينقر المتلقي وينتهي من الإعداد، يشرع الفيروس في إتلاف نظام الهاتف بعدة طرق ممكنة، وعادة ما يكون ذلك بالحذف السريع أو التفكيك.

4 الإعلانات غير المرغوب فيها: تشمل رسائل الإعلانات الاقتحامية MMS عادة أنواعاً مختلفة من الإعلانات عن أشياء، من قبيل إعلانات القروض والعقارات وعروض التدريب وغيرها. وتُرسل هذه الرسالة الاقتحامية إلى المتلقي دون إذن المتلقي أو دون أن يكون هذا الأخير مشتركاً في الخدمة. وعادة ما يكون بعض هذه الرسائل خادعاً وقد يحتوي على رابط إعلاني في الصورة أو الفيديو المرسل، وإذا قام المتلقي بالنقر على الصورة أو الفيديو، يعاد توجيه متصفح الويب إلى صفحة الإعلانات.

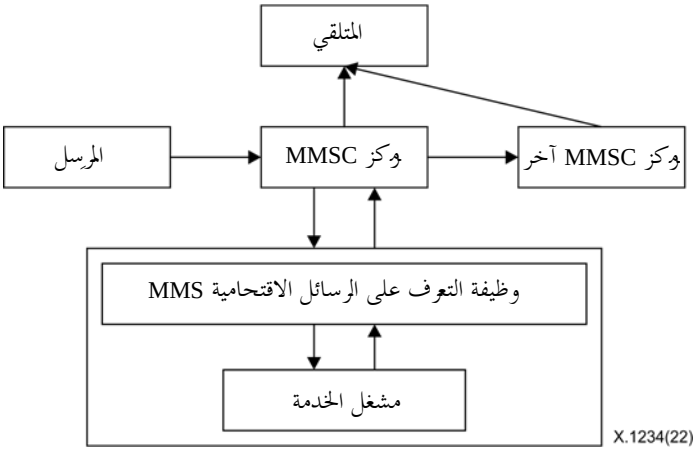
8 مبادئ توجيهية بشان الإطار التقني

1.8 الهيكل العام

كما هو مبين في الشكل 8-1، يرسل المرسِل رسالة الوسائط المتعددة إلى مركز MMSC ويقوم المتلقي بتنزيل رسالة الوسائط المتعددة من مركز MMSC، لذلك يخزن المركز MMSC جميع الرسائل MMS. ولهذا السبب، يوصى بنشر وظائف التعرف على الرسائل الاقتحامية MMS (MMSSIF) على مقربة من المركز MMSC.

لا يمكن لأي تكنولوجيا لمكافحة الرسائل الاقتحامية أن تضمن دقة بنسبة 100%، وتتطلب وظيفة MMSSIF أن يتم تشكيلها وإدارتها يدوياً خارج الخط، ولذلك، ينبغي إعداد مشغل الخدمة كما هو مبين في الشكل 8-1.

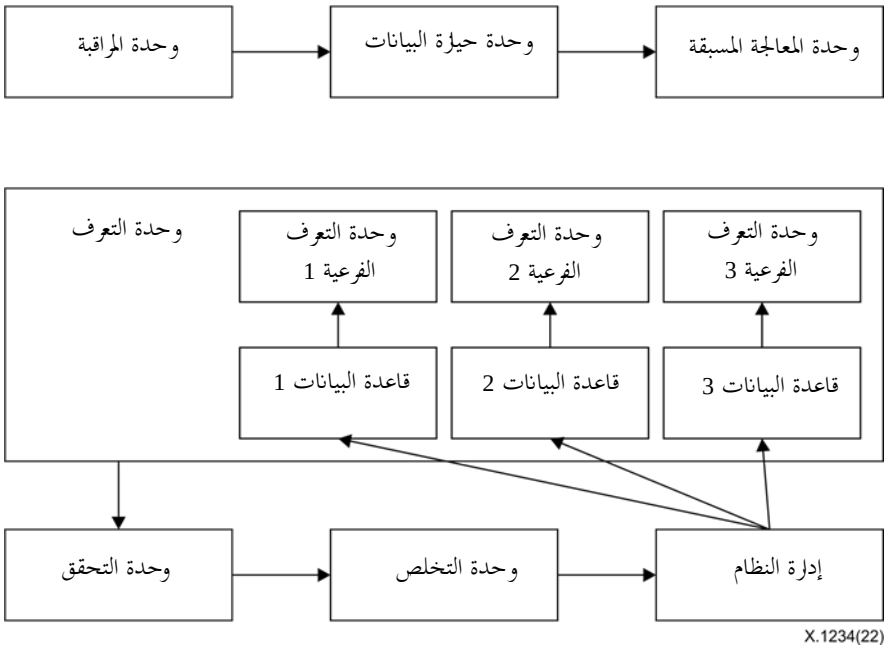
وفي الوقت نفسه، ينبغي تعديل سير عمل المركز MMSC الأصلي بحيث يرسل المركز الرسالة MMS إلى الوظيفة MMSSIF بدلاً من إعادة توجيهها إلى المتلقي أو المركز MMSC التالي مباشرة بعد تلقي الرسالة MMS. وتحدد الوظيفة MMSSIF ما إذا كانت الرسالة MMS اقتحامية أم لا، ومن ثم تقدم اقتراحات مقابلة إلى المركز MMSC. ووفقاً لهذه الاقتراحات، يحدد المركز ما إذا كان سيستمر في إرسال هذه الرسالة إلى المتلقي أو إلى المركز التالي.



الشكل 8-1 – الهيكل العام لمكافحة الرسائل الاقتحامية MMS

2.8 الهيكل العام لوظيفة التعرف على الرسائل الاقتحامية MMS (MMSSIF)

يشمل الهيكل المرجعي MMSSIF أساساً سبع وحدات تقابل وظائف مختلفة: المراقبة وحيازة البيانات والمعالجة المسبقة والتعرف والتحقق والتخلص وإدارة النظام. ويوصى بربط الوحدات المختلفة. وينبغي التنسيق فيما بينها وفقاً للقواعد أو السياسات المحددة في الاتفاقات ذات الصلة.



الشكل 8-2 – الهيكل المرجعي للوظيفة MMSSIF

في الشكل 8-2، تتلقى وحدة المراقبة رسالة الوسائط المتعددة من المركز MMSC وتحصل على رأسية رسالة الوسائط المتعددة هذه، بما في ذلك الموضوع ورقم هاتف المرسِل وعدد المرفقات وعنوان URL الخاص بهذه المرفقات وما إلى ذلك.

وتتلقى وحدة حيازة البيانات رسائل رأسية رسالة الوسائط المتعددة من وحدة المراقبة، ثم تقوم بتنزيل جميع المرفقات من العنوان URL.

وتتلقى وحدة المعالجة المسبقة جميع رسائل الخدمة MMS هذه من حيازة البيانات، بما في ذلك الرأسية وجميع المرفقات، ثم تقوم بتقييس الرسائل حسب القواعد. وقد تأتي الرسائل من رأسية أو متن الرسائل MMS، ويمكن أن تكون الرسائل في شكل نص، أو صورة أو فيديو أو صوت، وما إلى ذلك، ولذا، يوصى بأن تكون القواعد قواعد مركبة مثل "المصدر + نوع الرسالة + الرسالة".

وتتلقى وحدة التعرف الرسائل المقيّسة من وحدة المعالجة المسبقة وتبحث ما إذا كانت رسالة الوسائط المتعددة هذه رسالة اقتحامية باستخدام بعض التكنولوجيات، مثل القائمة السوداء والتعرف على النص والتعرف على الصور والتعرف على الفيديو وما إلى ذلك.

وتتلقى وحدة التحقق النتيجة المحتملة من وحدة التعرف وتصدر أحكاماً إضافية مثل التحديدات اليدوية من أجل تقليل إمكانية الإنذارات الخاطئة.

وتتلقى وحدة التخلص نتيجة التعرف من وحدة التحقق وتتخلص من رسالة الوسائط المتعددة التي تعتبر رسالة اقتحامية، مثلاً من خلال منع رسائل الوسائط المتعددة، وإرسال رسالة تنبيه إلى المقتحم، وما إلى ذلك. كما أنها ترسل رسالة الوسائط المتعددة الأصلية، وسجل التخلص ورقم هاتف المرسِل إلى وحدة إدارة النظام.

وتتلقى وحدة إدارة النظام السجلات من وحدة التخلص وتقوم بحفظ سجل العمليات وسجل النظام. كما أنها ترسل رقم هاتف المقتحم، والكلمات الرئيسية، والصور إلى قواعد البيانات المختلفة في وحدة التعرف من أجل تحديث قواعد البيانات.

3.8 المكونات الوظيفية للوظيفة MMSSIF

1.3.8 وحدة المراقبة

تشمل وظائف وحدة المراقبة ما يلي:

- مراقبة ما إذا كانت هناك رسالة MMS جديدة تُرسل من مركز MMSC؛
- تلقي تدفق البيانات الكامل لرسالة الوسائط المتعددة؛
- تحليل تدفق البيانات والحصول على رأسية رسالة الوسائط المتعددة؛
- إرسال الموضوع، ورقم هاتف المرسِل، وعدد المرفقات، وعنوان URL لتلك المرفقات ومتن الرسالة MMS إلى وحدة حيازة البيانات.

2.3.8 وحدة حيازة البيانات

تشمل وظائف وحدة حيازة البيانات ما يلي:

- تلقي الرسائل من وحدة المراقبة والعثور على عنوان URL لتلك المرفقات؛
- تنزيل جميع المرفقات؛
- إرسال جميع رسائل الخدمة MMS إلى وحدة المعالجة المسبقة، بما في ذلك رأسية ومتن الرسالة MMS الذي يتضمن جميع المرفقات.

3.3.8 وحدة المعالجة المسبقة

تشمل وظائف وحدة المعالجة المسبقة ما يلي:

- تلقي جميع الرسائل من وحدة حيازة البيانات؛
- التحقق من جميع المرفقات وتقدير ما إذا كانت نصاً، أو صورة أو صوتاً أو فيديو، إذ لا يُسمح إلا بإدراج نص أو صورة أو صوت أو فيديو في رسالة الوسائط المتعددة وفقاً لبروتوكول النقل MMS الحالي؛
- تصنيف الرسائل وفقاً لأنواع مختلفة وتقييس الرسائل حسب القواعد مثل القواعد المركبة "المصدر + نوع الرسالة + الرسالة"؛
- إرسال رسالة الوسائط المتعددة الأصلية، وجميع الرسائل المقيسة ورقم هاتف المرسِل إلى وحدة التعرف.

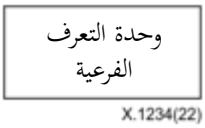
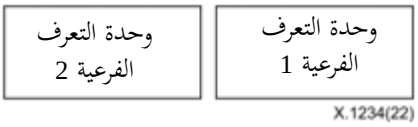
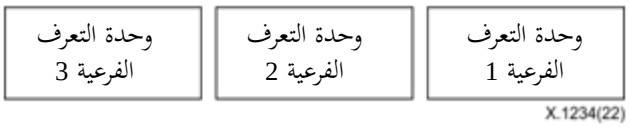
4.3.8 وحدة التعرف

تشمل وظائف وحدة التعرف ما يلي:

- بحث ما إذا كانت رسالة الوسائط المتعددة رسالة اقتحامية؛
- إرسال نتيجة التعرف إلى وحدة التحقق.

وهناك أساساً ثلاثة أنواع من تكنولوجيات التعرف وفقاً لأجزاء مختلفة من الرسالة MMS. ويستند النوع الأول إلى رقم الهاتف، مثل القائمة السوداء والقائمة البيضاء. أما الثاني فيستند إلى النص، مثل التعرف على النص. ويستند النوع الأخير إلى المرفقات مثل التعرف على الصور، وغير ذلك. وتبعاً للمتطلبات والخصائص المحددة لمورّد الخدمة، قد تنشر وحدة التعرف وحدة فرعية مختلفة وفقاً لنوع التكنولوجيات.

الجدول 8-1 – نموذج تشكيلة وحدة التعرف

النموذج	الوصف
النموذج 0	 يحتوي النموذج 0 على وحدة فرعية واحدة، ويستعمل نوعاً واحداً من تكنولوجيا التعرف.
النموذج 1	 النموذج 1 هو شكل يجمع بين الوحدة الفرعية 1 والوحدة الفرعية 2 المشكلتين معاً. ويمكن أن تكون الوحدة الفرعية 1 والوحدة الفرعية 2 أي نوعين من الأنواع الثلاثة.
النموذج 2	 النموذج 2 هو شكل يجمع بين الوحدة الفرعية 1 والوحدة الفرعية 2 والوحدة الفرعية 3 المشكّلة معاً.

في النموذج 1 والنموذج 2، يمكن حساب نتيجة التعرف بطرق مختلفة. فعلى سبيل المثال، في النموذج 1، تنشر وحدة التعرف الفرعية 1 التعرف على النص وتنشر وحدة التعرف الفرعية 2 التعرف على الصورة. وتعرّفت وحدة التعرف الفرعية 1 على أن رسالة الوسائط المتعددة رسالة اقتحامية، ولكن لم تتعرف وحدة التعرف الفرعية 2 على أن رسالة الوسائط المتعددة نفسها رسالة اقتحامية. ولذلك، فإن التعرّف على ما إذا كانت رسالة اقتحامية أم لا، يتطلب استراتيجية شاملة لوحدة التعرف. ويوصى بتشكيل الاستراتيجية وفقاً للاحتياجات والحالة الفعلية.

5.3.8 وحدة التحقق

تشمل وظائف وحدة التحقق ما يلي:

- تلقي النتائج المحتملة من وحدة التعرف؛
- إصدار مزيد من الأحكام مثل عمليات التحديد اليدوية.

6.3.8 وحدة التخلص

تشمل وظائف وحدة التخلص ما يلي:

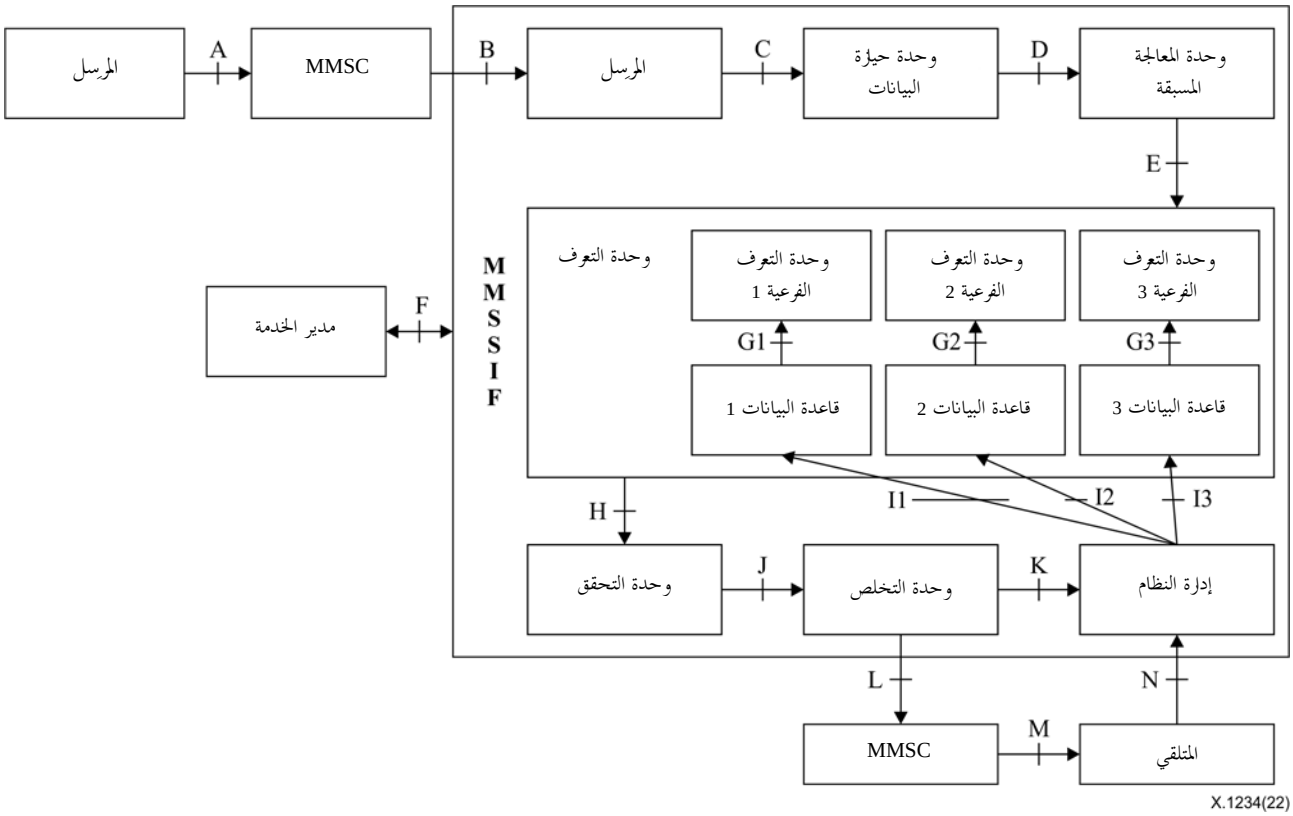
- تلقي النتائج من وحدة التحقق؛
- التخلص من الرسالة MMS وفقاً لنتيجة التعرف القادرة على الحكم على ما إذا كانت رسالة الوسائط المتعددة رسالة اقتحامية أم لا؛
- إرسال نتيجة التخلص إلى وحدة إدارة النظام إذا تم التعرف على رسالة الوسائط المتعددة كرسالة اقتحامية؛
- إرسال رسالة الوسائط المتعددة الأصلية إلى مركز MMSC إذا لم يتم التعرف على رسالة الوسائط المتعددة كرسالة اقتحاية.

7.3.8 وحدة إدارة النظام

تشمل وظائف وحدة إدارة النظام ما يلي:

- حفظ سجل العمليات وسجل النظام؛
- تحديث قواعد البيانات؛
- تلقي معلومات مرتدة من المستعملين.

4.8 نموذج مرجعي



الشكل 8-3 – نموذج مرجعي لمكافحة الرسائل الاقتحامية الموجهة عبر رسائل الوسائط المتعددة

يوجد السطح البيني A بين المرسِل والمركز MMSC. ويُستخدم السطح البيني A لإرسال رسالة الوسائط المتعددة إلى المركز MMSC. وقد تحقق ذلك بالفعل عندما بدأ مورّد الخدمة تقديم خدمة الرسائل متعددة الوسائط إلى المستعملين. ولا حاجة إلى تغييره في هذا النموذج.

ويوجد السطح البيني B بين المركز MMSC ووحدة المراقبة. وهو سطح بيني جديد يُستخدم لإرسال رسالة الوسائط المتعددة إلى وحدة المراقبة بدلاً من توجيهها إلى المتلقي أو إلى المركز MMSC التالي مباشرة.

ويوجد السطح البيني C بين وحدة المراقبة ووحدة حيازة البيانات. ويُستخدم لإرسال رأسية رسالة الوسائط المتعددة، ورقم هاتف المرسِل، والعنوان URL وغير ذلك من المعلومات التي تقوم وحدة المراقبة بتحليلها.

ويوجد السطح البيني D بين وحدة حيازة البيانات ووحدة المعالجة المسبقة. ويُستخدم لإرسال جميع الرسائل، بما في ذلك رسالة الوسائط المتعددة، والمتن والموضوع وجميع المرفقات وما إلى ذلك.

ويوجد السطح البيني E بين وحدة المعالجة المسبقة ووحدة التعرف. ويُستخدم لإرسال الرسائل المقيّسة من قبيل "المصدر + نوع الرسالة + الرسالة". وينبغي للسطح البيني E أن يدعم بروتوكول FTP وبروتوكول HTTP.

ويوجد السطح البيني F بين مشغل الخدمة والوظيفة MMSSIF. ويُستخدم لإرسال قواعد التشكيل وإحصاءات الرسائل الاقتحامية.

ويوجد السطح البيني G بين قاعدة البيانات والوحدة الفرعية. والسطح البيني G ليس سطحاً بينياً محدداً. ويمثل فئة من السطوح البينية بين قاعدة بيانات مختلفة ووحدة التعرف الفرعية المقابلة لها. ويُستخدم لإرسال الأرقام والنصوص والصور المشبوهة وغيرها والتي تتم مطابقتها في قواعد البيانات من أجل التعرف على الرسائل الاقتحامية.

ويوجد السطح البيني H بين وحدة التعرف ووحدة التحقق. ويُستخدم لإرسال النتائج المحتملة ورسالة الوسائط المتعددة الأصلية.

ويوجد السطح البيني I بين إدارة النظام وقاعدة البيانات. والسطح البيني I ليس سطحاً بينياً محدداً تماماً مثل السطح البيني G، ويمثل فئة من السطوح البينية بين قاعدة بيانات مختلفة وإدارة النظام.

ويوجد السطح البيني J بين وحدة التحقق ووحدة التخلص. ويُستخدم لإرسال نتيجة التعرف ورسالة الوسائط المتعددة الأصلية.

ويوجد السطح البيني K بين وحدة التخلص وإدارة النظام. ويُستخدم لإرسال رقم هاتف المرسِل، ونتيجة التعرف، والتخلص ورسالة الوسائط المتعددة الأصلية.

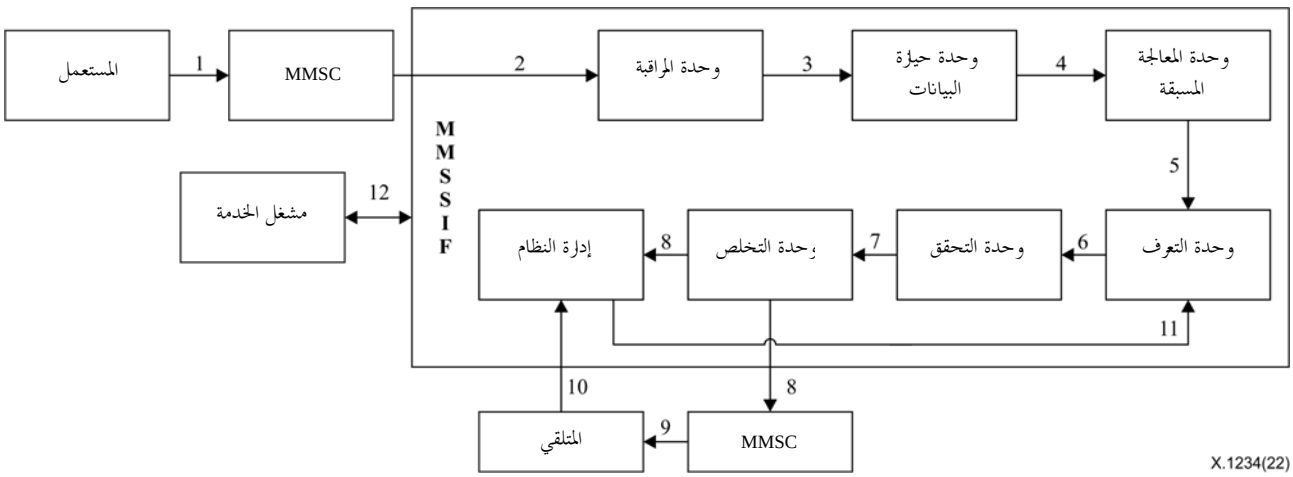
ويوجد السطح البيني L بين وحدة التخلص ومركز MMSC. ويُستخدم لإرسال رسالة الوسائط المتعددة الأصلية التي لم يتم التعرف عليها كرسالة اقتحامية.

ويوجد السطح البيني M بين مركز MMSC والمتلقي. ويُستخدم لإرسال رسالة الوسائط المتعددة إلى المتلقي. وقد تحقق ذلك بالفعل عندما بدأ مورّد الخدمة تقديم خدمة الرسائل متعددة الوسائط إلى المستعملين. ولا حاجة لتغييره في هذا النموذج.

ويوجد السطح البيني N بين المتلقي ونظام الإدارة. ويُستخدم لإرسال المعلومات المرتدة من المتلقي.

9 إجراءات العمل

يبين الشكل 9-1 أن مكافحة الرسائل الاقتحامية الموجهة عبر رسائل الوسائط المتعددة تتكون من اثني عشر إجراءً. وتشكل هذه الإجراءات نظاماً تكييفياً يسهم في تعظيم أداء النظام.



الشكل 9-1 – إجراءات معالجة مكافحة الرسائل الاقتحامية الموجهة عبر رسائل الوسائط المتعددة

الإجراء 1: إرسال رسالة الوسائل المتعددة إلى مركز MMSC

يُعدّ المرسّل محتوى رسالة الوسائط المتعددة، ورقم هاتف المتلقي ثم يرسل هذه الرسالة إلى مركز MMSC.

الإجراء 2: إعادة توجيه رسالة الوسائط المتعددة إلى وحدة المراقبة

يتلقى مركز MMSC رسالة الوسائط المتعددة من المركز ثم يعيد توجيهها إلى وحدة المراقبة مباشرة.

الإجراء 3: الحصول على رأسية رسالة الوسائط المتعددة

تراقب وحدة المراقبة ما إذا كانت هناك رسالة وسائط متعددة جديدة تُرسل من مركز MMSC طوال الوقت. وبمجرد وجود رسالة وسائط متعددة جديدة، تتلقى الوحدة تدفق البيانات الكامل لرسالة الوسائط المتعددة، وتحلل تدفق البيانات وتحصل على رأسية رسالة الوسائط المتعددة، بما في ذلك الموضوع ورقم هاتف المرسِل وعدد المرفقات وعنوان URL الخاص بهذه المرفقات. وعندئذ، ترسل وحدة المراقبة جميع الرسائل إلى وحدة حيازة البيانات.

الإجراء 4: تنزيل جميع المرفقات

تتلقى وحدة حيازة البيانات الرسائل من وحدة المراقبة، وتحدد عنوان URL الخاص بتلك المرفقات، وتقوم بتنزيل جميع المرفقات. وبعد الحصول على جميع رسائل MMS، ترسلها إلى وحدة المعالجة المسبقة.

الإجراء 5: تقييس رسائل الوسائط المتعددة

تتحقق وحدة المعالجة المسبقة من جميع المرفقات وتحدد ما إذا كانت نصاً أو صورة أو صوتاً أو مقطع فيديو بعد تلقي الرسائل من وحدة حيازة البيانات. وإذا كانت جميع الرسائل قانونية، تقوم وحدة المعالجة المسبقة بتصنيف الرسائل وفقاً لأنواع مختلفة، وتقييسها حسب القواعد. وبعد ذلك ترسل رسالة الوسائط المتعددة الأصلية وجميع الرسائل المقيّسة ورقم هاتف المرسِل إلى وحدة التعرف.

الإجراء 6: تحليل رسالة الوسائط المتعددة

تحلل وحدة التعرف ما إذا كانت رسالة الوسائط المتعددة رسالة اقتحامية أم لا وفقاً لتكنولوجيات مختلفة، يتم نشرها في النظام العملي. وبعد ذلك ترسل النتيجة المحتملة إلى وحدة التحقق. وباستثناء بعض التكنولوجيات المحددة، تحتاج وحدة التعرف إلى بعض الاستراتيجيات الشاملة للحصول على النتيجة النهائية المحتملة.

الإجراء 7: إصدار مزيد من الأحكام

تصدر وحدة التحقق المزيد من الأحكام بعد تلقي النتائج المحتملة من وحدة التعرف وترسل نتيجة التعرف إلى وحدة التخلص.

الإجراء 8: التخلص من رسالة الوسائط المتعددة

تتخلص وحدة التخلص من رسالة الوسائط المتعددة وفقاً لنتيجة التعرف. وإذا تم التعرف على رسالة الوسائط المتعددة على أنها رسالة اقتحامية تتخلص وحدة التخلص منها وفقاً لقواعد مثل حظر الرسالة MMS، وإرسال تحذير إلى المقتحم وما إلى ذلك. وترسل أيضاً إلى وحدة إدارة النظام الرسالة MSS الأصلية وسجل التخلص ورقم هاتف المرسِل. ولن يتلقى المتلقي الرسالة MMS هذه. وإذا لم يتم التعرف على رسالة MMS كرسالة اقتحامية، ترسل وحدة التخلص رسالة الوسائط المتعددة الأصلية إلى مركز MMSC

الإجراء 9: إرسال رسالة الوسائط المتعددة إلى المتلقي

يرسل مركز MMSC رسالة الوسائط المتعددة إلى المتلقي. وفي بعض الأحيان، يرسل رسالة الوسائط المتعددة إلى مركز MMSC آخر ومن ثم يرسلها إلى المتلقي. وهذا الإجراء مطابق للإجراء السابق قبل وجود وظيفة MMSSIF.

الإجراء 10: المعلومات المرتدة من المتلقين

يمكن للمتلقين، كضحايا محتملين للرسائل الاقتحامية، إرسال تعليقات طواعية إلى وحدة إدارة الخدمة. ولذلك تعتبر مشاركة المتلقين مفيدة في مكافحة الرسائل الاقتحامية مكافحة تتسم بالفعالية والكفاءة. وبالتالي، يوصى بأن تستخدم إدارة النظام تعليقات المتلقين عند وضع الحلول من أجل مكافحة الرسائل الاقتحامية.

الإجراء 11: تحديث قواعد البيانات

تحفظ وحدة إدارة النظام سجل التشغيل وسجل النظام ورسائل الوسائط المتعددة الأصلية. وتقوم بتحديث قواعد البيانات أيضاً، وفقًا للعينات ورقم الهاتف والكلمات الرئيسية وما إلى ذلك.

الإجراء 12: ضبط تدابير مكافحة الرسائل الاقتحامية

يقوم مشغل الخدمة، طبقاً لإحصاءات الرسائل الاقتحامية وتقرير التحليل الواردة من وظيفة MMSSIF، بتقييم أداء الوظيفة MMSSIF لتقديم تحسينات محتملة. واستناداً إلى نتيجة التقييم، قد يتم تعديل التدابير والاستراتيجيات وقد يعدّل مشغل الخدمة آليات التعاون في وحدة التعرف.

10 مبادئ توجيهية بشأن التكنولوجيات الرئيسية

تستطيع رسالة الوسائط المتعددة أن تنقل العديد من رسائل الوسائط المتعددة بما في ذلك الصور والنصوص ومقاطع الفيديو والصوت وما إلى ذلك. وبالتالي، فإن تكنولوجيات التعرف الرئيسية لمكافحة الرسائل الاقتحامية الموجهة عبر رسائل الوسائط المتعددة تشمل بشكل رئيسي التعرف على الصور، والتعرف على النص، والتعرف على الفيديو، والتعرف على الصوت، وما إلى ذلك.

1.10 قائمة مراشيح الرسائل الاقتحامية

تتضمن قائمة مراشيح الرسائل الاقتحامية القائمة السوداء والقائمة البيضاء والقائمة الغامضة. وينبغي لمقدمي الخدمة تشكيل الوظيفة MMSSIF لتسجيل النشاط المشبوه أو تشكيله تلقائياً (كحظر رسائل الوسائط المتعددة المشبوهة، والسماح برسائل الوسائط المتعددة العادية) لاستخدام القائمة السوداء أو القائمة البيضاء. وينبغي لمقدمي الخدمة أيضاً تحديث القوائم لضمان توافر الوظائف MMSSIF وتشغيلها المستقر. وعند اكتشاف حالات شاذة لرقم هاتف غير مدرج في القائمة، ينبغي تحويل رقم الهاتف إلى عملية استعراض يدويو لإجراء تقييم كامل.

2.10 التعرف على الصور

تستخرج تقنية التعرف على الصورة ميزة تمثيل الصورة أولاً وتنشئ قاعدة بيانات للقيمة الذاتية للصورة. ويصبح الكشف عن رسالة اقتحامية بعد ذلك مشكلة تصنيف ثنائية في حيز الميزة يمكن حلها عن طريق التعلم الآلي التقليدي. أو بعبارة أبسط، إذا تمت مطابقة القيمة الذاتية لصورة رسالة الوسائط المتعدد في قاعدة البيانات، تُعرّف الرسالة على أنها رسالة اقتحامية. وتعتمد هذه الطريقة على جودة قاعدة بيانات القيمة الذاتية للصورة.

3.10 التعرف على النص

يشمل التعرف على النص أساساً التعرف على الكلمات الرئيسية والتعرف الدلالي. وينشئ التعرف على الكلمات الرئيسية أولاً قاعدة بيانات الكلمات الرئيسية. إذا تضمن محتوى نص رسالة الوسائط المتعددة كلمات رئيسية مدرجة في قاعدة بيانات الكلمات الرئيسية، يتم التعرف على الرسالة على أنها رسالة اقتحامية، وبالإضافة إلى ذلك، يمكن للتعرف على النص بناء نماذج منطقية بولانية ونموذج مكان المتجه، وبعد التدريب، يتم الحصول على نموذج التعرف الذي يمكن أن يحسن دقة التعرف على النص. وتعتمد هذه الطريقة على جودة قاعدة بيانات الكلمات الرئيسية.

وفي بعض الأحيان، يكون المقتحمون على درجة عالية من الابتكار في تجنب الكشف عن هويتهم. إذ باستطاعتهم مثلاً تزييف البريد الإلكتروني العادي وتوزيع محتواه عشوائياً لتجنب اكتشاف الكلمات الرئيسية لمراشيح الرسائل الاقتحامية. ولذلك، استناداً إلى التعرف على الكلمات الرئيسية، من الفعال للغاية استخدام التعرف الدلالي لتحقيق التعرف الثانوي (مثل نهج معالجة اللغة الطبيعية بناءً على التعرف الدلالي الجزئي) الذي قد يقلل بشكل كبير من المعدل الإيجابي الخاطئ.

4.10 التعرف على الفيديو

عادة ما يبدأ التعرف على الفيديو بإنشاء قاعدة بيانات للعينات، ثم مقارنة فيديو رسالة الوسائط المتعددة بعينات فيديوية واحدة تلو الأخرى لتقييم ما إذا كان مقطع الفيديو رسالة اقتحامية أم لا. ويمكن تحديد ذلك أيضاً عن طريق استخراج الأرتال الرئيسية للفيديو. وتشمل العمليات الرئيسية ما يلي: فك تشفير الفيديو ومعالجته كمجموعة من الصور ثم أخذ عينات من تلك الصور، وتحديد الصور التي تم أخذ عينات منها استناداً إلى تقنية التعرف على الصور، وأخيراً الحصول على نتيجة التعرف على الفيديو من نتيجة التحليل الشامل للصور التي أُخذت عينة منها.

5.10 التعرف على الصوت

يمكن تنفيذ التعرف على الصوت بالاقتران مع تكنولوجيا التعرف التلقائي على الصوت (ASR). والغرض من هذه التكنولوجيا تمكين الحواسيب من "إملاء" الكلام المستمر الكامل أو نطق الكلمات أو العبارات الرئيسية بواسطة متحدثين مختلفين، وتحويل "الصوت" إلى "نص". وبالإضافة إلى ذلك، لتحديد بيانات صوتية متشابهة أو متطابقة، تُستخرج خصائص طيفية، وتُحسب بصمة صوتية قصيرة وقوية. وبالتالي، يمكن للتكنولوجيا ASR "التعرف" على بعض الكلمات الرئيسية المعينة في الصوت، وتحديد ما إذا كان الصوت رسالة اقتحامية أم لا.

6.10 تعليقات المستعملين النهائيين

تنطبق تعليقات المستعملين النهائيين وإرشادات التنفيذ المرتبطة بها وغيرها من المعلومات المحددة في البند 5.8 من التوصية [ITU-T X.1231] وفي الملحق A بالتوصية [ITU-T X.1247].

يقوم بعض المستعملين النهائيين بحذف الرسالة الاقتحامية MMS عند تلقيها مباشرة، بينما يقوم عدد قليل منهم بالإبلاغ عن هذه الرسائل من خلال القناة الرسمية لملاحظات العملاء. وتعتمد فعالية هذه الطريقة على حماس المستعملين النهائيين ومبادرتهم. وتُشجع المشاركة الفعالة للمستعملين النهائيين لمكافحة الرسائل الاقتحامية MMS مكافحة تتسم بالفعالية والكفاءة.

بيبليوغرافيا

[b-ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[b-ITU-T X.1241] Recommendation ITU-T X.1241 (2008), *Technical framework for countering email spam.*

[b-ITU-T X.1242] Recommendation ITU-T X.1242 (2009), *Short message service (SMS) spam filtering system based on user-specified rules.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*

[b-ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2022